MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

July/August 2025

Benefits of Cyber-security Awareness Programmes

Cyber-security awareness programmes provide informative training sessions on cyber-threats and cyber-security best practices. These programmes aim to educate employees and organisations about the importance of maintaining a secure online environment and the potential risks associated with cyber-attacks.

These programmes can offer several benefits to organisations, such as:

- **Improved employee understanding of cyber-security risks and best practices—**Extensive training provides employees with vital information about data breaches and how to prevent them. This can reduce the likelihood of successful phishing attacks, social engineering tactics and other cyber-security incidents.
- **Faster incident response and mitigation due to employee preparedness**—Once employees are equipped with the knowledge to respond to cyber-attacks, they can act more swiftly if one occurs. This may reduce an incident's spread and impact, which, in turn, can lessen needed response times and lower associated costs.
- **Enhanced customer trust**—Compliance with industry regulations and standards may instil trust in clients. A cyber-security awareness programme demonstrates an organisation's commitment to data protection.
- **Potential insurance cost savings**—Insurance providers may offer more favourable premiums to businesses with cyber-security awareness programmes because such training may reduce the likelihood of breaches, resulting in a lower chance of needing to file an insurance claim related to the losses.

When implementing cyber-security awareness programmes, organisations should consider their unique cyber-vulnerabilities and tailor the training to address these. They should also leverage a range of training methods (eg simulations, real-world examples and gamification) to enhance employee engagement.

The Importance of Cyber-insurance for SMEs

While cyber-attacks can severely affect organisations of any size, small and medium-sized enterprises (SMEs) are particularly vulnerable to the associated financial and reputational fallout. According to cyber-security researcher Cybersecurity Ventures, 60% of small businesses shut down within six months of experiencing a data breach or cyber-attack. SMEs are increasingly becoming prime targets for cyber-criminals, who often exploit vulnerabilities in smaller companies' software to gain a foothold in larger businesses through supply chain attacks. Further increasing their susceptibility to cyber-threats, SMEs typically have smaller budgets for cyber-security and fewer IT staff to implement and manage effective security measures.

Fortunately, cyber-insurance can financially protect SMEs from the devastating consequences of cyber-attacks by covering data restoration and rectification costs, legal liability from personal or confidential data breaches, lost profits and other expenses. It may also include access to IT forensics, legal experts, public relations advisors and other specialists often lacking in SMEs, helping to expedite their recovery.

While investing in cyber-security measures and robust insurance may be challenging for SMEs with scant resources, recovering from a cyber-attack can be far costlier. Contact us today for further business insights and robust insurance solutions.

Mitigating VPN Vulnerabilities

A virtual private network (VPN) is a type of technology that uses an encrypted connection to route internet traffic through a remote server, granting a user access to certain digital services while masking their online activity. Connecting to a VPN establishes a safe tunnel between a user's device and the internet, making it seem as though they are browsing from the server's original location and protecting their data from being intercepted by malicious parties. Over the years, VPNs have become a crucial cyber-security tool for many organisations, particularly those that permit employees to work from different locations and use public wi-fi networks.

Yet, hackers are increasingly exploiting VPN vulnerabilities to carry out cyber-attacks, often taking advantage of outdated encryption protocols, weak authentication mechanisms, unpatched software and coding errors. Upon exploiting an organisation's VPN vulnerabilities, threat actors may be able to infiltrate its larger IT infrastructure, ultimately disrupting critical operations, creating possible supply chain complications and compromising confidential data.

According to a report by IT company Cybersecurity Insiders, almost half (45%) of organisations experienced at least one attack that exploited VPN vulnerabilities in a 12-month period. As such, it's imperative for organisations to clearly understand the cyber-security challenges tied to VPNs and take steps to mitigate them.

Considering the potentially severe ramifications of VPN vulnerabilities, it's essential for organisations to leverage effective risk management techniques. Here are some best practices for organisations to consider:

1. **Conduct risk assessments.** Organisations should review and document their unique cyber-risks, taking into consideration their key operations, essential services, sensitive data and digital assets. From there, organisations can better determine what type of VPN will be most effective for their particular circumstances.
2. **Select a trusted service provider.** Organisations should carefully research different VPN service providers and choose one with a solid reputation and a commitment to cyber-security. The best VPN service providers typically provide built-in encryption features and have no-logs policies, meaning they won't store any data regarding users' online activity.
3. **Enable security features.** Organisations should enable any security features available to strengthen their VPNs, including anti-malware programmes, adblockers, multifactor authentication protocols and data leak prevention tools. In addition to the VPN software itself, these security features should be updated regularly. If possible, organisations should consider enabling automatic software and security updates or deploying patch management solutions to stay on track with such updates.
4. **Monitor network activity and perform audits.** Various threat detection tools (eg endpoint detection and response solutions) can help organisations closely monitor their VPN connections and identify any unusual network activity in real time. In conjunction with such tools, organisations should also perform routine security audits to help detect any ongoing VPN vulnerabilities (eg misconfigured code) and make adjustments as needed.
5. **Educate staff**. Organisations should educate their staff about proper VPN use. This includes creating strong passwords; using safe devices; and only accessing data, systems and services deemed critical to fulfilling their job roles.
6. **Consider alternatives**. In some cases, VPNs may not be worth the risks they pose to organisations. Under these circumstances, organisations should consider alternative remote access solutions, such as zero-trust network access, virtual desktop infrastructure, secure access service edge, software-defined perimeters or privileged access management tools.

Contact us today for additional cyber-risk management guidance.

The content of this publication is of general interest and is not intended to apply to specific circumstances or jurisdiction. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice from their own legal counsel. Further, the law may have changed since first publication and the reader is cautioned accordingly.